REMARKS

Favorable reconsideration of this application, in light of the following discussion, is respectfully requested.

Claims 11-21 are currently pending. No claims have been amended herewith.

In the outstanding Office Action, Claims 11 and 21 were rejected under 35 U.S.C. § 102(a) as being anticipated by U.S. Patent Application Publication No. 2003/0097563 to Moroney et al. (hereinafter "Moroney"); Claims 12-14 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Moroney in view of U.S. Patent Application Publication No. 2002/0051539 to Okimoto et al. (hereinafter "Okimoto"); and Claims 15-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Moroney in view of U.S. Patent No. 5,748,732 to Le Berre et al. (hereinafter "Le Berre").

RESPONSE TO ARGUMENTS

The Office Action dated December 28, 2009, states that the Examiner respectfully disagrees with the arguments presented in the Amendment filed September 10, 2009, regarding Moroney and the other cited references. However, the Office Action does not explain why the Examiner disagrees with Applicants' interpretation of those references. Rather, the Office Action appears to simply cite several sections of Moroney without discussing how those sections relate to the specific features of the claims. Accordingly, it is respectfully requested that the Examiner *set forth the reasons that each of the previously presented arguments, further discussed below, were found not to be persuasive* in accordance with MPEP § 707.07(f).

REJECTION UNDER 35 U.S.C. § 102

Previously presented Claim 11 is directed to a method for distribution of scrambled data and/or services to at least one master terminal and to at least one slave terminal linked with the master terminal, the method comprising:

> transmitting by a central management module to the master terminal a first secret code S_m and transmitting by the central management module to each slave terminal a second secret code S_s;
>
> storing the first secret code S_m in the master terminal and the second secret code S_s in each slave terminal and,
>
> for each use of a slave terminal by a user,
>
> checking whether the first secret code S_m has previously been stored in the slave terminal,
>
> when the first secret code S_m has previously been stored in the slave terminal,
>
>> checking whether the first secret code S_m is in a biunique relationship with the second secret code S_s,
>
> when the first secret code S_m has not previously been stored in the slave terminal,
>
>> inviting said user to enter the first secret code S_m in said slave terminal, and
>>
>> checking whether the first secret code S_m entered by the user in the slave terminal is in a biunique relationship with the second secret code S_s,
>
> authorizing the reception of the scrambled data and/or services by the slave terminal, when the first secret code S_m is in a biunique relationship with the second secret code S_s, and
>
> prohibiting the reception of the scrambled data and/or services by the slave terminal, when the first secret code S_m is not in a biunique relationship with the second secret code S_s.

Regarding the rejection of Claim 11 under 35 U.S.C. § 102(a), the Office Action apparently cites the Moroney reconfiguration of set-top boxes, which are each equipped with two cryptographic keys (a unit key and an authentication key), and verification that the set-top boxes are connected together for teaching all the features of Claim 11.[1]

However, it is respectfully submitted that Moroney fails to disclose checking whether the first secret code S_m has previously been stored in the slave terminal, when the first secret code S_m has previously been stored in the slave terminal, checking whether the first secret code S_m is in a biunique relationship with the second secret code S_s, when the first secret code S_m has not previously been stored in the slave terminal, inviting said user to enter the first secret code S_m in said slave terminal, and checking whether the first secret code S_m entered by the user in the slave terminal is in a biunique relationship with the second secret code S_s, authorizing the reception of the scrambled data and/or services by the slave terminal, when the first secret code S_m is in a biunique relationship with the second secret code S_s, and prohibiting the reception of the scrambled data and/or services by the slave terminal, when the first secret code S_m is not in a biunique relationship with the second secret code S_s. Rather, Moroney simply discusses that a slave box is linked to a master box with a physical communication link so that if the physical link is severed, e.g., if an attempt is made to move the slave box to another household to provide unauthorized service in that household, the slave box is programmed to stop working when it can no longer communication with the master box.[2] Further, with respect to the cited unit and authentication keys, Moroney simply discusses that the unit key is used for reconfiguration, and the authentication key is shared between a master-slave pair to verify that they have not been separated.[3] Moroney does not disclose that the detection of whether a physical link is severed or the use of unit and authentication keys involve checking, inviting, authorizing, and prohibiting steps, as defined in Claim 11.

[1] See Office Action dated December 28, 2009, pages 4 and 5.
[2] See Moroney, paragraph [0018].
[3] Id. at paragraph [0031].

For example, with respect to the step of checking whether the first secret code S_m has previously been stored in the slave terminal, Moroney simply discusses that since a master-slave pair share the same authentication key which is unknown outside of the two set-top boxes and the billing software, it has the necessary cryptographic values to verify that the two set-top boxes are linked together. Moroney discusses that this is accomplished using a "ping" protocol. After the elapse of some fixed time interval, e.g., 15 minutes, the slave sends a pseudo-randomly generated value to the master. The master does a cryptographic signature of the received value via a message authentication code (MAC) using the shared authentication key, and sends the result back to the slave. The slave verifies whether the correct signature was obtained, including the use of the correct pseudo-randomly generated value sent, to determine whether to continue normal operation.[4] Moroney does not disclose ***checking*** whether the authentication key, or a first secret code S_m, ***has previously been stored*** in the slave set-top box.

Further, with respect to the steps of, when the first secret code S_m has not previously been stored in the slave terminal, inviting said user to enter the first secret code S_m in said slave terminal, and checking whether the first secret code S_m entered by the user in the slave terminal is in a biunique relationship with the second secret code S_s, as cited in the Office Action, Moroney discusses

> Each set-top is equipped with two cryptographic keys: a unit key and an authentication key. The unit key is used for reconfiguration, and the authentication key is shared between a master-slave pair **to verify that they have not been separated**. Both keys are delivered to the set-tops in encrypted form, so that neither the installer, customer, nor authorized agent is aware of the true key values. The initial ("provisioning") keys are provided during the manufacturing process of the set-tops.

That is, Moroney simply describes a method for (permanently) linking two set-top boxes (the master and the slave) and for detecting any subsequent disconnection or blockage of

[4] See Moroney, paragraph [0037].

communication between the set-top boxes.[5] This "linking" is pre-configured by an authorized agent which provides to both set-top boxes the same authentication key[6] known only to the set-top boxes and the billing software. The master-slave pair has the necessary cryptographic values to verify that the two set-top boxes are linked together.[7] The link between the slave and master set-top boxes in Moroney ***is not performed by a user***.

On the other hand, for a non-limiting example, there is no pre-configuration process of a pair of master-slave set-top boxes in the claimed invention. Rather, when a user wishes to receive data and/or service on one or more supplementary receiver terminals, the user just enters the first secret code S_m, previously provided by the operator, in the supplementary terminals. The introduction of the first secret code S_m in the supplementary terminals results in the master-slave configuration. There is no need for a pre-configuration process by a specific authorized agent. This configuration is performed by the user depending on need.

Accordingly, Applicants respectfully traverse the rejection of Claim 11 (and dependent Claim 21) as being anticipated by Moroney.

REJECTION UNDER 35 U.S.C. § 103

Regarding the rejections of dependent Claims 12-14 under 35 U.S.C. § 103(a), it is respectfully submitted that Okimoto fails to remedy the deficiencies of Moroney, as discussed above. Moreover, the Office Action does not cite Okimoto for those deficiencies. Accordingly, it is respectfully submitted that Claims 12-14 patentably define over any proper combination of Moroney and Okimoto.

Regarding the rejections of dependent Claims 15-17 under 35 U.S.C. § 103(a), it is respectfully submitted that Le Berre fails to remedy the deficiencies of Moroney, as discussed

[5] See Moroney, paragraph [0027].
[6] Id. at paragraph [0036].
[7] Id. at paragraph [0037].

above. Accordingly, it is respectfully submitted that Claims 15-17 patentably define over any proper combination of Moroney and Le Berre.

Previously presented Claim 18 is directed to a scrambled data and/or service distribution system for at least one master terminal and at least one slave terminal, each equipped with a security processor, the system comprising:

> a central subscriber management module;
>
> an entitlement management message generator;
>
> a scrambling platform;
>
> means for attributing to the master terminal a first secret code S_m, and to each slave terminal a second secret code S_s; and
>
> control means for authorizing reception of the data and/or services by a slave terminal only when the first secret code S_m is previously stored in the slave terminal and when the first secret code S_m entered in the slave terminal is in a biunique relationship with the second secret code S_s.

Regarding the rejection of Claim 18 under 35 U.S.C. § 103(a), as noted above, Moroney fails to disclose the checking, inviting, authorizing, and prohibiting steps of Claim 11. Thus, Moroney fails to disclose the control means of Claim 18. Further, it is respectfully submitted that Le Berre fails to remedy the deficiencies of Moroney, as discussed above, and it is noted that the Office Action does not cite Le Berre for those deficiencies.

Thus, no matter how the teachings of Moroney and Le Berre are combined, the combination does not teach or suggest the control means of Claim 18. Accordingly, it is respectfully submitted that Claim 18 (and all associated dependent claims) patentably defines over any proper combination of Moroney and Le Berre.

CONCLUSION

Thus, it is respectfully submitted that independent Claims 11 and 18 (and all associated dependent claims) patentably define over Moroney, Okimoto, and Le Berre.

Consequently, in light of the above discussion, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Should the Examiner deem that any further action is necessary to place this application in even better form for allowance, the Examiner is encouraged to contact Applicants' undersigned representative at the below listed telephone number.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Gregory J. Maier
Attorney of Record
Registration No. 25,599

Johnny Ma
Registration No. 59,976

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)
3611745_1.DOC